Універсальність, скритність, багатоваріантність форм програмно-апаратної реалізації, радикальність дії, достатній вибір часу і місця застосування, нарешті, економічність роблять інформаційну зброю надзвичайно небезпечною: вона легко маскується під засоби захисту, наприклад, інтелектуальної власності; вона дозволяє навіть вести наступальні дії анонімно, без оголошення війни.

Нормальна життєдіяльність суспільства цілком визначається рівнем розвитку, якістю функціонування і безпекою інформаційного середовища. Виробництво і управління, оборона і зв'язок, транспорт і енергетика, фінанси, наука і освіта, засоби масової інформації – все залежить від інтенсивності інформаційного обміну, повноти, своєчасності, достовірності інформації.

Саме інформаційна інфраструктура суспільства – мішень інформаційної зброї. Але в першу чергу інформаційна зброя націлена на збройні сили, підприємства оборонного комплексу, структури, відповідальні за зовнішню і внутрішню безпеку держави.

Темпи вдосконалення інформаційної зброї перевищують темпи розвитку технологій захисту. Тому задача нейтралізації інформаційної зброї повинна розглядатися як одна з пріоритетних в забезпеченні національної безпеки держави.

Для того щоб захиститися від загрози застосування інформаційної зброї перш за все необхідна оцінка загрози. Потрібний також періодичний аналіз геостратегічної ситуації з погляду вірогідності виникнення інформаційної війни. Ці оцінки і аналіз можуть служити основою для вироблення національної концепції протидії (нейтралізації) загрозі такої війни.

Таким чином, створення єдиного глобального інформаційного простору, що є природним результатом розвитку світової науково-технічної думки і вдосконалення комп'ютерних інформаційних технологій, створює передумови до розробки і застосування інформаційної зброї. Ефективне володіння інформаційною зброєю і засобами захисту від нього стає однією з головних умов забезпечення національної безпеки держави в XXI столітті.

Список літератури.

1. Панарин И. Н. Технология информационной войны/ И.Н. Панарин.–М.:“КСП+”, 2003.–320 с.
2. Прохожев А. А., Турко Н. И. Основы информационной войны, 1995.

УДК 004.9:32.019.51

Модель поведінки держави в умовах проявів ознак інформаційної експансії, агресії, війни

Доренський О.П., викладач
Кіровоградський національний технічний університет, м. Кіровоград

Інформація, яка визначається як сигнали або відомості, сприйняті приймачем та перетворені у сигнали керування [1], сьогодні активно використовується як ефективний інструмент досягнення суспільно-політичних, економічних, геополітичних цілей держави, а за допомогою сучасних інформаційних технологій перетворена на потужну зброю масового ураження. Адже боротьба держав в інформаційному просторі ведеться за зони політичного й економічного впливу, джерела сировини, ринки збуту й території, а всередині країни – за владу, власність, політичний вплив, можливість маніпулювати настроями й поведінкою громадян [2]. Означене призвело до появи й активного ведення війн нового покоління – інформаційних (ІВ), під якими розуміють проведення широкомасштабних інформаційних

дій, що застосовуються сторонами, які знаходяться у протиборстві, направлених проти соціальних та інформаційно-технічних систем держави з метою одержання інформаційної переваги над противником [3]. Вони стали несиловим засобом забезпечення державами власних інтересів та вирішальним фактором в досягненні результатів.

На сьогодні ІВ є ефективним засобом оволодіння ресурсами за допомогою механізмів агітації, пропаганди й інформаційного протистояння [2], що здійснюється у формах (ступенями) інформаційної експансії, інформаційної агресії та інформаційної війни [4, 9].

Відповідно до класифікації [5] ІВ є війнами сьомого покоління. Її поява стала наслідком наступних чинників:

– розвиток засобів обчислювальної техніки і комунікації [2];

– розвиток прикладної психології у сфері вивчення поведінки людей та управління їх мотиваціями [2, 6];

– глобалізація та масштабна інформатизація суспільства.

Предметом інформаційної війни є впливи на об'єкти. Серед багатьох їх різновидів під час ведення ІВ ключовим є інформаційний [7], надефективність якого забезпечують:

– активне впровадження у фахову діяльність й повсякденне життя людей електронних інфокомунікаційних систем, соціальних мереж, мобільних пристроїв тощо;

– інтеграція у життя й виникнення стійкої залежності сучасної людини від інформаційно-телекомунікаціних, мережевих, мобільних засобів тощо, які стають основним джерелом інформації, а, отже, формують думку, світогляд та поведінку громадськості.

Водночас, спостерігається стрімке вдосконалення засобів ведення інформаційної боротьби. Першочергово це стосується інформаційної зброї, яка призначена для боротьби з комп'ютерними мережами і системами управління. До сучасної інформаційної зброї входить сукупність спеціально організованої інформації та інформаційних технологій, що дозволяє цілеспрямовано змінювати, знешкоджувати, копіювати, блокувати інформацію, долати системи захисту, здійснювати дезінформацію, пошкоджувати функціонування носіїв інформації, інфокомунікаційних систем та мереж [8].

Отже, з означеного випливає, що актуальною задачею є постійний моніторинг відповідними органами держави проявів ознак інформаційної експансії, агресії, війни [9] або їх гібридів, яку слід сприймати як пряму загрозу національній безпеці та невідкладно вживати належних заходів і застосування засобів інформаційної протидії й захисту. Таким чином, метою роботи є розроблення моделі адекватної поведінки держави (її відповідних органів) на ранніх стадіях інформаційної експансії, агресії, війни або їх гібридних форм.

Задля захисту інформаційного простору держави в умовах проявів ознак інформаційної експансії, агресії або війни слід вжити заходів нейтралізації й знищення інформаційного ресурсу противника та захисту власного інфоресурсу. Реалізувати означене можливо за допомогою інформаційно-ударної операції [10]. Її базовими задачами є:

– забезпечення інформаційної переваги шляхом активного впливу на системи державного і військового управління противника та на джерела інформаційних загроз;

– введення противника в оману стосовно операції, яка проводиться;

– зниження морально-психологічної стійкості та бойового духу особового складу противника;

– протидія негативному інформаційному впливу противника.

Інформаційно-ударна операція проводиться на основі [11]:

– використання сучасних інформаційних та телекомунікаційних засобів, технологій, соціальних мереж тощо;

– застосування військових засобів;

– демонстрація вогневої могутності сучасної зброї, передислокація військ;

– висвітлення та характеристика в засобах масової інформації об'єктів ураження;

– організація потоків біженців та провокації громадських зіткнень;

– цілеспрямований вплив на суспільну думку щодо несприйняття противника, блокування кордонів, введення ембарго на поставку військової та інших видів

продукції противника;

– масове використання безпілотних літальних апаратів та високоточної зброї;
– висвітлення подій у світових інформаційно-телекомунікаційних мережах;
– знищення військово-стратегічних цілей.

Отже, за результатами дослідження запропоновано та в доповіді презентується модель поведінки держави в умовах проявів ознак інформаційної експансії, агресії, війни або їх гібридів. Її сутність полягає у здійсненні постійного моніторингу інформаційного простору, виявлення ознак інформаційного противника та невідкладне проведення інформаційно-ударної операції з метою протидії й захисту власних ресурсів на ранніх стадіях інформаційної експансії, агресії або війни. Означене дасть істотну перевагу у випадку ведення ІВ, можливість мінімізувати витрати на інформаційне протистояння, унеможливлення часткової або повної втрати політичного стану, ресурсів, а також забезпечення захисту суспільства, національного інтересу й держави в цілому.

Список літератури

1. Притула А.В. Природа інформації та її визначення / А.В. Притула, В.Я. Решетник // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій : IV Міжнар. наук.-прак. конф., 24-26 кві, 2008 р. : тези доп. – Запоріжжя, 2008. – С. 114-115.

2. Шумка А.В. Інформаційно-мережева війна – нова форма міждержавного протиборства початку XXI ст. / А.В. Шумка, П.П. Черник // Військово-науковий вісник. – 2013. – Вип. 19. – С. 243-255.

3. Медведєв В.К. Сучасна інформаційна війна та її обрис / Медведєв В.К., Кучеренко Ю.Ф., Гузько О.М. // Системи озброєння і військова техніка. – 2008. – № 1(13). – С. 52-54.

4. Пілат М. Інформаційні впливи та інформаційні війни: сутність понять та їхній взаємозв'язок в інформаційну епоху / Марина Пілат // Вісник Львівського університету. – 2013. – Вип. 32. – С. 185-190.

5. Слипченко В. Природа войны: вчера, сегодня, завтра / В.Слипченко. – М.: Третий Рим, 2004. – 196 с.

6. Сенченко О. Новітні війни з використанням інформаційно-психологічної зброї / Оксана Сенченко // Вісник Книжкової палати. – 2014. – № 8. – С. 1-6.

7. Воробйова І.В. Інформаційно-психологічна зброя як самостійний засіб ведення інформаційно-психологічної війни / І.В. Воробйова // Системи озброєння і військова техніка. – 2010. – № 1(21). – С. 141-144.

8. Кучеренко Ю.Ф. Погляди на ведення інформаційної боротьби в сучасних війнах / Кучеренко Ю.Ф., Гордієнко В.М., Гузько О.М. // Системи озброєння і військова техніка. – 2011. – № 3(27). – С. 108-111.

9. Мануйло А. В. Государственная информационная политика в условиях информационно-психологической войны. / А.В. Манойло, А.И. Петренко, Д.Б. Фролов. – М.: Горячая линия, 2003. – 541 с.

10. Гриняев С. Концепция ведения информационной войны в некоторых странах мира / Сергей Гриняев // Зарубежное военное обозрение. – 2002. – №2. – С. 11-16.

11. Войтко О.В. Передумови створення концепції інформаційної війни в еру новітніх технологій / О.В. Войтко // Сучасні інформаційні технології у сфері безпеки та оборони. – 2013. – № 3(18). – С. 99-100.

УДК 004.056.55

Інформаційні війни: поняття, мета, завдання та їх значення

Кліпа О.С., курсант 4 курсу
Науковий керівник – Безрученко В.С., канд. фіз.-мат. наук, доцент
Національний університет державної податкової служби України, м. Ірпінь

Інформаційна війна – використання і управління інформацією з метою набуття конкурентоздатної переваги над супротивником.

Інформаційна війна може включати в себе:

- збір тактичної інформації,